securonix DATASHEET

Insider Intent Agent

DETECT INTENT BEFORE IT BECOMES A BREACH

Most insider threat tools only detect what users do — not why they do it. Traditional rule- and regex-based approaches fail to capture tone, sentiment, behavioral drift, or emerging risks tied to AI-assisted workflows. As employees rely more heavily on AI platforms such as Microsoft Copilot, ChatGPT, and Google Gemini, intent now emerges earlier, inside prompts, queries, and contextual signals that legacy systems cannot see.

The Securonix Insider Intent Agent changes that.

Powered by advanced language models, behavioral analytics, and the Securonix Agentic Mesh, it uncovers early indicators of insider risk — from stress and disengagement to attempts to hide activity or misuse confidential data in AI tools. By correlating communicative signals with identity, activity, and data movement, the Insider Intent Agent provides clear, explainable insights that help analysts prioritize true risk and act before impact.

Why Intent Matters Now

Traditional Approaches Miss Early Warning Signs

Regex- and keyword-based insider risk tools over-alert on harmless terms while missing subtle cues — changes in tone, linguistic markers of distress, or indirect references to high-risk actions. They also lack visibility into AI workflows where employees increasingly create, summarize, and manipulate sensitive data.

AI Platform Telemetry Creates a New Visibility Gap

Without prompt-level insight into AI interactions, organizations cannot detect:

- Sensitive data placed into AI tools
- Attempts to bypass policy or obfuscate activity
- AI-assisted data exfiltration patterns
- High-risk sentiment shifts preceding misconduct

How the Insider Intent Agent Works

Intent-Based Analytics

Moves beyond static keyword detection to identify behavioral and linguistic cues including stress, hostility, obfuscation or disengagement.

Behavior and Communication Baselines

Continuously learns how users and entities normally behave and communicate, profiling deviations across access, activity, tone, and sentiment in both structured and unstructured data.

AI Interaction Intelligence

Ingests telemetry from platforms such as Microsoft Copilot, ChatGPT, and Gemini — including prompt content, metadata, and sentiment — enabling visibility into intent expressed within AI-assisted workflows. Securonix is the first insider risk solution to fuse enterprise telemetry with AI interaction intelligence.

Contextual Correlation

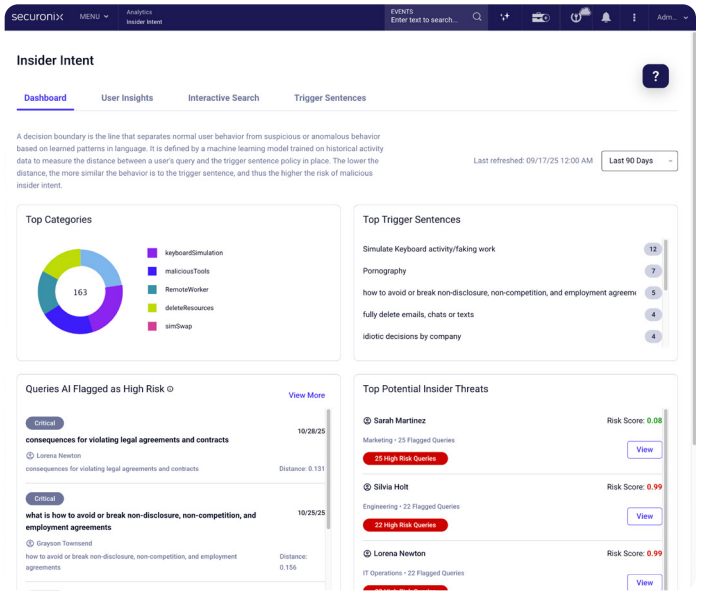
Enriches intent signals with asset sensitivity, peer comparisons, and threat intelligence to prioritize risk based on real business impact.

Risk Scoring & Prioritization

Scores each behavioral pattern using contextual, linguistic, and activity-based inputs — surfacing only the highest-risk users for immediate review.

Analyst-Ready Narrative Summaries

Transforms complex correlations into clear, plain-language summaries and recommended next steps — giving analysts immediate clarity on what is happening and why it matters.



Adaptive Learning

Continuously refines risk detection based on analyst feedback and evolving user behavior — improving precision and reducing false positives over time.

Cross-Agent Collaboration in the Agentic Mesh

Works with Search, Noise Control, and Response Agents across the Agentic Mesh ensuring that intent detections flow into investigation and containment workflow with full context and auditability. This ensures every insider-risk decision is contextualized, explainable, and aligned with SOC governance.

Cut the Noise and Focus on Real Risk

Operational Efficiency

Intent-based detection dramatically reduces false positives and directs analysts toward threat that truly matter.

Faster Investigations

Plain-language summaries and correlated context shorten investigation time from hours to minutes.

Trusted, Explainable Outcomes

Every detection includes an explanation of why it was triggered and how it maps to enterprise policy — building analyst, compliance, and executive confidence.

Continuous Accuracy

Adaptive models evolve with feedback and environmental change, ensuring insider-risk detection accuracy improves over time.

Compliance Assurance and AI Governance Readiness

Delivers governed, auditable detections aligned with insider-risk, data-protection, and regulatory mandates.

What the Insider Intent Agent Detects

Toxic Workplace & Grievances

Discontent, hostility, or perceived injustice — early markers of disengagement or malicious insider activity.

Obfuscation or Evasion Behavior

References to encryption, hiding activity, or bypassing controls.

Isolation, Burnout, or Distress

Psychological signals that correlate with susceptibility to external manipulation or policy violations.

High Stress or Anxiety Indicators

Stress-driven decision-making that can lead to accidental or intentional data exposure.

Flight Risk Indicators

Job hunting, external offer discussions, or negotiation signals that often precede data theft or exfiltration attempts.

AI-Assisted Sensitive Activity Detects employees using AI systems to:

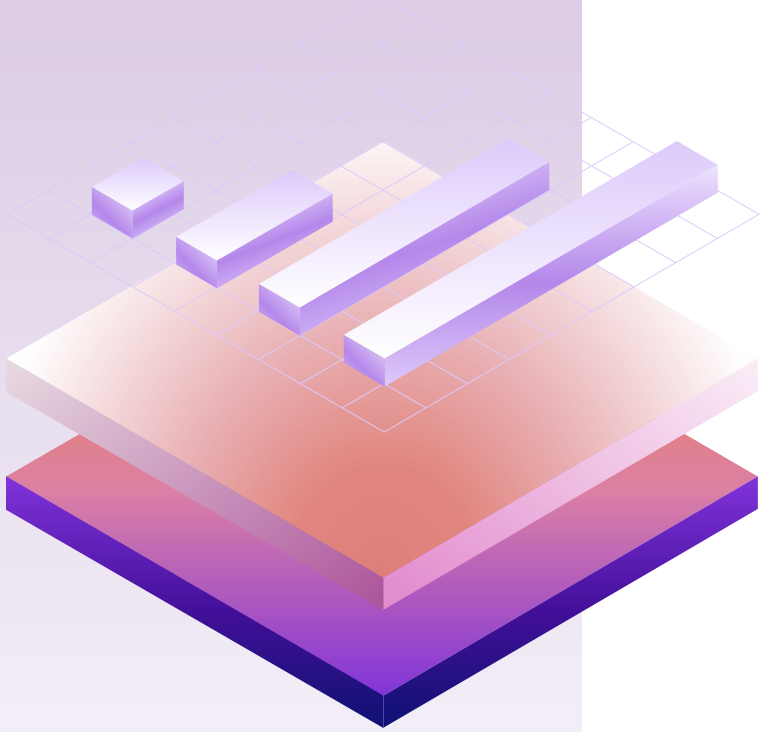
- Summarize confidential data
- Draft content based on proprietary information
- Generate code or queries using sensitive IP
- Search for ways to evade controls

Proven Results, Trusted by the Industry

Securonix has been recognized as a **6x Leader in the Gartner® Magic Quadrant™ for SIEM and achieved 193% ROI in the Forrester TEI Study.**

The Securonix Agentic Mesh is a governed ecosystem of AI-driven agents that collaborate to automate, explain, and secure the SOC.

The Insider Intent Agent works within this ecosystem to share findings, context, and reasoning with peers such as Search, Noise Control, and Response.



Uncover Insider Intent Before It Becomes a Breach.

Visit **securonix.com** or contact sales@securonix.com.